UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/500,131	06/25/2004	Richard C Madter	1679-52/JLW	7371

38735 7590 09/27/2006

DIMOCK STRATTON LLP
20 QUEEN STREET WEST SUITE 3202, BOX 102
TORONTO, ON M5H 3R3
CANADA

EXAMINER	
TRUJILLO, JAMES K	

ART UNIT	PAPER NUMBER
2116	

DATE MAILED: 09/27/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/500,131	MADTER ET AL.	
	Examiner	Art Unit	
	James K. Trujillo	2116	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *9/27/04*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *092704*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The office acknowledges the receipt of the following and placed of record in the file:

2. Claims 1-20 are presented for examination.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-3 and 7-13 and rejected under 35 U.S.C. 103(a) as being unpatentable over Mirov et al., U.S. Patent 6,138,236 in view of Cooper et al., U.S. Patent 5,805, 882 (cited in IDS).

5. Regarding claim 1, Mirov teaches a boot method for use in a mobile device having FLASH memory storing boot instructions, having internal memory comprising the steps of:

a. reading a key value from a security location in the FLASH memory (authentication section and digital signature in flash PROM, col. 3, lines 56-65, col. 4, lines 8-17 and figure 2);

b. comparing the key value to a predetermined security value stored in the internal memory (comparing verification hash with data hash, col. 4, lines 18-26 and col. 5, lines 6-15); and

Mirov does not explicitly disclose selectively polling the serial port for activity based on the result of the comparison.

Cooper teaches selectively polling a port if a flash ROM is corrupted (col. 3, lines 18-26). Cooper further provides the advantage of allowing a flash ROM to be updated to a known valid state even if the computer system is unable to boot up because of among other things the flash ROM is corrupted (col. 3, lines 18-26).

It would have been obvious to one of ordinary skill in the art, having the teachings of Mirov and Cooper before them at the time the invention was made to modify Mirov to include selectively polling serial a port based on a comparison of a key value if a flash ROM is corrupted as taught by Cooper.

One of ordinary skill in the art would have been motivated to make this modification in order to achieve the advantage of allowing a flash ROM to be updated to a known valid state even if the computer system is unable to boot. Mirov teaches that a comparison will fail if a flash ROM is corrupted (col. 4, lines 18-26). Further, Cooper teaches polling a parallel port, however it would have been obvious to one of ordinary skill in the art to modify the teaching of Cooper to be used in a serial port because type of port is an obvious modification know to those of ordinary skill in the art. Modifying Cooper to use a serial port would provide the same advantages as those used in a parallel port.

6. Regarding claim 2, Mirov together with Cooper taught the method according to claim 1, as described above. Cooper teaches that the polling is performed if the Flash ROM is corrupted. Mirov teaches that a Flash ROM is corrupted if the key value does not match the predetermined security value. Therefore, together they teach that the polling is performed if the key value does not match the predetermined security value.

7. Regarding claim 3, Mirov together with Cooper taught the method according to claim 1, as described above. Mirov teaches further comprising the step of jumping to a boot location in FLASH memory to execute instruction stored therein (permitted to execute, col. 4, lines 18-25).

8. Regading claim 7, Mirov together with Cooper taught the method according to claim 1, as described above. Mirov further teaches wherein the predetermined security value is stored in a Boot ROM located in a mobile device (hand held systems, col. 3, lines 48-55).

9. Regarding claim 8, Mirov together with Cooper taught the method according to claim 1, as described above. Mirov further teaches wherein the step of reading is performed in response to a reset command (wherein a startup is interpreted to include a reset, col. 3, line 36). Cooper also teaches further teaches wherein the step of reading is performed in response to a reset command (col. 3, lines 13-27).

10. Regarding claim 9, Mirov teaches an apparatus for use in a mobile device having a serial port, comprising:

a. a first internal memory means having a predetermined security value stored therein (Public Key in section 45 of Boot Prom 18, figure 2);

b. a second memory means having a security location for storing a key value (signature in section 55 of Boot Prom 18, figure 2); and

c. a processor in communication with the first and second memory means for comparing a key value stored in the security location to the predetermined security value (CPU 12, figure 1),

Mirov does not explicitly disclose selectively polling the serial port for activity based on the result of the comparison.

Cooper teaches selectively polling a port if a flash ROM is corrupted (col. 3, lines 18-26). Cooper further provides the advantage of allowing a flash ROM to be updated to a known valid state even if the computer system is unable to boot up because of among other things the flash ROM is corrupted (col. 3, lines 18-26).

It would have been obvious to one of ordinary skill in the art, having the teachings of Mirov and Cooper before them at the time the invention was made to modify Mirov to include selectively polling serial a port based on a comparison of a key value if a flash ROM is corrupted as taught by Cooper.

One of ordinary skill in the art would have been motivated to make this modification in order to achieve the advantage of allowing a flash ROM to be updated to a known valid state even if the computer system is unable to boot. Mirov teaches that a comparison will fail if a flash ROM is corrupted (col. 4, lines 18-26). Further, Cooper teaches polling a parallel port, however it would have been obvious to one of ordinary skill in the art to modify the teaching of Cooper to be used in a serial port because type of port is an obvious modification know to those of ordinary skill in the art. Modifying Cooper to use a serial port would provide the same advantages as those used in a parallel port.

11. Regarding claim 10, Mirov together with Cooper taught the apparatus according to claim 9, as described above. Mirov further teaches wherein the first internal memory means comprises a BootROM (col. 2, lines 53-64 and col. 3, liens 56-65).

12. Regarding claim 11, Mirov together with Cooper taught the apparatus according to claim 9, as described above. Mirov further teaches wherein the second memory means comprises a FLASH memory (col. 3, liens 56-65).

13. Regarding claim 12, Mirov together with Cooper taught the apparatus according to claim 9, as described above. Mirov further teaches comprising a reset means in communication with the processor for initiating reset process (wherein a startup is interpreted to include a reset, col. 3, line 36). Cooper also teaches further comprising a reset means in communication with the processor for initiating reset process (col. 3, lines 13-27).

14. Regarding claim 13, Mirov together with Cooper taught the apparatus according to claim 9, as described above. Mirov further teaches wherein the processor compares the key value and said predetermined security value in response to initiation of a reset process (col. 3, lines 14-35).

15. Claims 4-6 and 14-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Applicant's Admitted Prior Art (AAPA) in view of Mirov and Cooper.

16. Regarding claim 4, AAPA teaches a boot method for use in a mobile device having FLASH memory storing boot instructions, having internal memory, and having a serial port (figure 1), comprising the steps of:

the step of downloading code into internal SRAM located in the mobile device (paragraph [0005]).

AAPA does explicitly disclose reading a key value from a security location in the FLASH memory; comparing the key value to a predetermined security value stored in the

internal memory; and selectively polling the serial port for activity based on the result of the comparison; wherein the polling is performed if the key value does not match the predetermined security value; and wherein the downloading is in response to a detection of serial port activity.

Mirov teaches a boot method for use in a mobile device having FLASH memory storing boot instructions, having internal memory comprising the steps of:

reading a key value from a security location in the FLASH memory (authentication section and digital signature in flash PROM, col. 3, lines 56-65, col. 4, lines 8-17 and figure 2);

comparing the key value to a predetermined security value stored in the internal memory (comparing verification hash with data hash, col. 4, lines 18-26 and col. 5, lines 6-15).

Mirov is in the same field of endeavor as that of AAPA in that both are directed toward booting a computer. Mirov further provides the advantage of easily authenticating firmware (col. 1 line 65 through col. 2, line 3 and col. 5, lines 33-50).

It would have been obvious to one of ordinary skill in the art, having the teachings of AAPA and Mirov before them at the time the invention was made to modify the system of AAPA to include reading a key value and comparing the key value as taught by Mirov.

One of ordinary skill in the art would have been motivated to make this modification in order to provide the advantage of easily authenticating firmware in view of Mirov.

Cooper teaches selectively polling a port if a flash ROM is corrupted (col. 3, lines 18-26). Cooper further provides the advantage of allowing a flash ROM to be updated to a known valid state even if the computer system is unable to boot up because of among other things the flash ROM is corrupted (col. 3, lines 18-26).

It would have been obvious to one of ordinary skill in the art, having the teachings of AAPA and Cooper before them at the time the invention was made to modify the system and in particular the serial port of AAPA to include selective polling the as taught by Cooper.

One of ordinary skill in the art would have been motivated to make this modification in order to achieve the advantage of allowing a flash ROM to be updated to a known valid state even if the computer system is unable to boot. Mirov teaches that a comparison will fail if a flash ROM is corrupted (col. 4, lines 18-26). Further, Cooper teaches polling a parallel port, however it would have been obvious to one of ordinary skill in the art to modify the teaching of Cooper to be used in a serial port because type of port is an obvious modification know to those of ordinary skill in the art. Modifying Cooper to use a serial port would provide the same advantages as those in a parallel port.

17. Regarding claim 5, AAPA together with Mirov and Cooper taught the method according to claim 4, as described above. Cooper teaches further comprising the step of executing an instruction in the downloaded code (booting the computer col. 11, lines 1-18).

18. Regarding claim 6, AAPA together with Mirov and Cooper taught the method according to claim 4, as described above. Cooper teaches further comprising the step of jumping to a boot location in FLASH memory to execute boot instructions stored therein (inherent in booting the computer col. 11, lines 1-18).

19. Regarding claim 18, AAPA teaches a method for bootup of a computing device, the computing device comprising a serial port and internal memory comprising FLASH memory

(FLASH memory 18) and a BootROM memory comprising BootROM code (BootROM 14, figure 1) comprising the steps of:

a. executing instructions stored in the BootROM code (paragraph [0004]);

b. polling the serial port for activity (paragraph [0005]);

c. downloading new code into internal memory through the serial port in response to a detections of serial port activity (paragraph [0005]).

d. transferring execution to instructions in the new code (paragraph [0005]).

AAPA does not explicitly disclose the BootROM to read a key value from a security location in the FLASH memory, the key value being independent of the contents of the FLASH memory; the BootROM code to compare the key value to a predetermined security value stored in the BootROM memory; on the condition that the comparison shows a match between the key value and the predetermined security value, executing instructions in the BootROM code to transfer execution to instructions stored in a boot location in the FLASH memory; and wherein the polling, the downloading and the transferring is on the condition that the comparison shows a mismatch between the key value and the predetermined security value.

Mirov teaches a BootROM (section 45 of PROM 18, figure 2) to read a key value from a security location in a FLASH memory (signature 57 in section 55 of PROM 18, figure), the key value being independent of the contents of the FLASH memory (wherein the signature is interpreted to be independent from the contents of the FLASH memory because does not depend on the contents of the FLASH memory) and the BootROM code to compare the key value to a predetermined security value stored in the BootROM memory (inherent in order to calculate and

compare the hash, col. 4, lines 14-26) and on condition that the comparison shows a match between the key value, executing instruction in the BootROM code to transfer execution to instructions in a boot location in a FLASH memory (unsecured code is permitted to execute, col. 4, line 20-22). Mirov further provides the advantage of easily authenticating firmware (col. 1 line 65 through col. 2, line 3 and col. 5, lines 33-50).

It would have been obvious to one of ordinary skill in the art, having the teachings of AAPA and Mirov before them at the time the invention was made to modify the BootROM and FLASH memory of AAPA to include a key value and a predetermined security value and comparing them as taught by Mirov.

One of ordinary skill in the art would have been motivated to make this modification in order to provide the advantage of easily authenticating firmware in view of Mirov.

Cooper teaches on the condition that the comparison shows a mismatch between the a key value and a predetermined security value:

polling a port for activity (polling a port if a Flash ROM is corrupted, col. 3, lines 18-26);

downloading new code in response to a detection of port activity (updating the Flash ROM, col. 3, lines 18-26); and

transferring execution to instruction in the new code (Cooper suggests this when updating the Flash ROM).

Cooper provides the advantage of allowing a flash ROM to be updated to a known valid state even if the computer system is unable to boot up because of among other things the flash ROM is corrupted (col. 3, lines 18-26).

It would have been obvious to one of ordinary skill in the art, having the teachings of AAPA and Cooper before them at the time the invention was made to modify the system and in particular the serial port of AAPA to include selective polling the as taught by Cooper.

One of ordinary skill in the art would have been motivated to make this modification in order to achieve the advantage of allowing a flash ROM to be updated to a known valid state even if the computer system is unable to boot. Mirov teaches that a comparison will fail if a flash ROM is corrupted (col. 4, lines 18-26). Further, Cooper teaches polling a parallel port, however it would have been obvious to one of ordinary skill in the art to modify the teaching of Cooper to be used in a serial port because type of port is an obvious modification know to those of ordinary skill in the art. Modifying Cooper to use a serial port would provide the same advantages as those in a parallel port.

20. Regarding claims 19 and 20, AAPA together with Mirov and Cooper taught the claimed method therefore together they also teach the claimed program product and claimed apparatus.

21. Regarding claim 14, AAPA together with Mirov and Cooper taught the claimed method, as per claim 18, therefore together they teach the claimed apparatus according to claim 9, for the same reasons. AAPA further teaches wherein the first internal memory is located on an ASIC (BootROM 14 in ASIC 2, figure 1).

22. Regarding claim 15, AAPA together with Mirov and Cooper taught the claimed method, as per claim 18, therefore together they teach the claimed apparatus according to claim 9, for the same reasons. AAPA further teaches wherein a processor is located on an ASIC (processor 4, figure 1).

23. Regarding claim 16, AAPA together with Mirov and Cooper taught the claimed method, as per claim 18, therefore together they teach the claimed apparatus according to claim 9, for the same reasons. AAPA further teaches wherein a processor comprises a microcontrol unit connected to the serial port (DSP 4 together with MCU 6, figure 1).

24. Regarding claim 17, AAPA together with Mirov and Cooper taught the claimed method, as per claim 18, therefore together they teach the claimed apparatus according to claim 9, for the same reasons. AAPA further teaches wherein the processor comprises a digital signal processor connected the second memory means (DSP is coupled to FLASH 18, figure 1).

Conclusion

25. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Pat. No. 6,263,431 to Lovelace et al. teaches comparing keys during booting.

U.S. Pat. No. 6,775,778 to Laczko, Sr., et al. teaches comparing keys between a boot rom and a flash memory in order execute an application.

U.S. Pat. Appl. Pub. No. 2005/0081071 to Huang et al., teaches comparing a key in flash memory prior to booting.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to James K. Trujillo whose telephone number is (571) 272-3677. The examiner can normally be reached on M-F (8:00 am - 5:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Lynne Browne can be reached on (571) 272-3670. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

James K. Trujillo
Primary Examiner
Technology Center 2100